

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2 0 0 4 年 5 月 1 8 日

出 願 番 号

Application Number:

特 願 2 0 0 4 - 1 4 7 4 2 2

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2 0 0 4 - 1 4 7 4 2 2

出 願 人

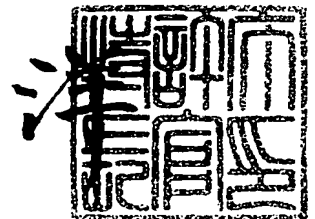
Applicant(s):

松下電器産業株式会社

2 0 0 5 年 5 月 2 0 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



BEST AVAILABLE COPY

【官 公 庁】	付 訂 願
【整理番号】	2047960086
【提出日】	平成16年 5月18日
【あて先】	特許庁長官殿
【国際特許分類】	G09C 1/00
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】	張 毅波
【特許出願人】	
【識別番号】	000005821
【氏名又は名称】	松下電器産業株式会社
【代理人】	
【識別番号】	100097445
【弁理士】	
【氏名又は名称】	岩橋 文雄
【選任した代理人】	
【識別番号】	100103355
【弁理士】	
【氏名又は名称】	坂口 智康
【選任した代理人】	
【識別番号】	100109667
【弁理士】	
【氏名又は名称】	内藤 浩樹
【手数料の表示】	
【予納台帳番号】	011305
【納付金額】	16,000円
【提出物件の目録】	
【物件名】	特許請求の範囲 1
【物件名】	明細書 1
【物件名】	図面 1
【物件名】	要約書 1
【包括委任状番号】	9809938

【請求項 1】

第 1 の通信装置と第 2 の通信装置との間で認証処理を行った上で前記第 1 の通信装置と前記第 2 の通信装置との間で通信を行う通信方法であって、

前記第 2 の通信装置の公開鍵情報と、前記第 2 の通信装置を特定するための ID 情報とを含む認証要求メッセージを前記第 1 の通信装置に送信する認証要求ステップと、

前記第 1 の通信装置が受信した前記認証要求メッセージに含まれる、前記第 2 の通信装置を特定するための ID 情報と、前記認証要求メッセージを受信した際の通信路を特定する情報とを表示する第 1 の表示ステップと、

前記第 2 の通信装置が送信した前記認証要求メッセージに含まれる、前記第 2 の通信装置を特定するための ID 情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とを表示する第 2 の表示ステップと、

前記第 1 の表示ステップと、前記第 2 の表示ステップで表示された前記第 2 の通信装置を特定するための ID 情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とが一致しているかどうかを確認する第 1 の確認ステップと、

前記第 1 の確認ステップにおいて、前記第 2 の通信装置を特定するための ID 情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とが一致していると判断した場合に、前記第 1 の通信装置の公開鍵情報と、前記第 1 の通信装置を特定するための ID 情報とを含む認証応答メッセージを前記第 2 の通信装置に送信する認証応答ステップと

、
前記第 2 の通信装置が受信した前記認証応答メッセージに含まれる、前記第 1 の通信装置を特定するための ID 情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する第 3 の表示ステップと、

前記第 1 の通信装置が送信した前記認証応答メッセージに含まれる、前記第 1 の通信装置を特定するための ID 情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する第 4 の表示ステップと、

前記第 3 の表示ステップと、前記第 4 の表示ステップで表示された前記第 1 の通信装置を特定するための ID 情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とが一致しているかどうかを確認する第 2 の確認ステップ

とで構成されることを特徴とする通信方法。

【請求項 2】

前記認証要求ステップにおいて、認証要求メッセージはデジタル署名情報を更に含み、

前記第 1 の表示ステップにおいて、前記認証要求メッセージに含まれるデジタル署名情報を復号した結果、前記第 2 の通信装置の署名であると確認した場合に、前記第 2 の通信装置を特定するための ID 情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とを表示し、

前記認証応答ステップにおいて、認証応答メッセージはデジタル署名情報を更に含み、

前記第 3 の表示ステップにおいて、前記認証応答メッセージに含まれるデジタル署名情報を復号した結果、前記第 1 の通信装置の署名であると確認した場合に、前記第 1 の通信装置を特定するための ID 情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する

ことを特徴とする請求項 1 記載の通信方法。

【請求項 3】

前記認証要求メッセージを送信する際の通信路を特定する情報及び、前記認証応答メッセージを送信する際の通信路を特定する情報は、伝送に使用された無線チャネル情報であることを特徴とする請求項 1 または 2 記載の通信方法。

【請求項 4】

前記認証要求メッセージを送信する際の通信路を特定する情報は、前記第 2 の通信装置の公開鍵情報であり、

前記認証応答メッセージを送信する際の通信路を特定する情報は、前記第 1 の通信装置

ことを特徴とする請求項 1 または 2 記載の通信方法。

【請求項 5】

前記認証応答ステップにおいて、前記認証応答メッセージを前記第 2 の通信装置の公開鍵情報で暗号化する

ことを特徴とする請求項 1 または 2 記載の通信方法。

【請求項 6】

前記第 1 の通信装置を特定するための ID 情報及び前記第 2 の通信装置を特定するための ID 情報は、通信路設定を行うたびに都度生成する乱数である

ことを特徴とする請求項 1 または 2 記載の通信方法。

【請求項 7】

前記第 2 の確認ステップにおいて、前記第 1 の通信装置を特定するための ID 情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とが一致していると判断した場合に、前記第 2 の通信装置が、自身の生成した乱数を含む共通秘密鍵生成要求メッセージを前記第 1 の通信装置に送信する共通秘密鍵生成要求ステップと、

前記共通秘密鍵生成要求メッセージを受信した前記第 1 の通信装置が、自身の生成した乱数を含む共通秘密鍵生成応答メッセージを前記第 2 の通信装置に送信する共通秘密鍵生成応答ステップと、

前記第 1 の通信装置が、前記共通秘密鍵生成要求メッセージに含まれる乱数を用いて演算を行い、共通秘密鍵を生成し、前記第 2 の通信装置が、前記共通秘密鍵生成応答メッセージに含まれる乱数を用いて演算を行い、共通秘密鍵を生成する共通秘密鍵生成ステップを更に含むことを特徴とする請求項 1 または 2 記載の通信方法。

【請求項 8】

相手通信装置との間で認証処理を行った上で前記相手通信装置との間で通信を行う通信装置であって、

自装置の公開鍵及びプライベート鍵ペアを作成する公開鍵・プライベート鍵生成手段と

前記公開鍵・プライベート鍵作成手段が生成した公開鍵情報と、自装置を識別するための ID 情報とを少なくとも含む送信メッセージを生成し、前記相手通信装置に送信する送信手段と、

前記相手通信装置が送信した送信メッセージを受信し、前記相手通信装置が送信した送信メッセージに含まれる前記相手通信装置の公開鍵情報と、前記相手通信装置を識別するための ID 情報とを取り出す受信手段と、

自装置が前記相手通信装置から送信メッセージを受信した場合、前記受信手段が取り出した前記相手通信装置を識別するための ID 情報と、前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報とを表示する機能と、自装置が前記相手通信装置に送信メッセージを送信した場合、自装置が送信した送信メッセージに含まれる、自装置を特定するための ID 情報と、前記送信手段が送信メッセージを送信する際の通信路を特定する情報とを表示する機能とを有する表示手段と、

認証を許可するかどうかを入力する入力手段

とを有することを特徴とする通信装置。

【請求項 9】

入力されたデータを暗号化し、その結果をデジタル署名として出力するデジタル署名手段と、

前記相手通信装置から受信した前記相手通信装置の公開鍵、或いは自装置のプライベート鍵、或いは前記相手通信装置と共有する共通秘密鍵を用いて入力されたデータを暗号化する暗号化手段と、

前記相手通信装置から受信した前記相手通信装置の公開鍵、或いは自装置のプライベート鍵、或いは前記相手通信装置と共有する共通秘密鍵を用いて入力されたデータを復号化する復号化手段と、

入力されたデータに対して一方向ハッシュ関数を実行するハッシュ関数手段

を更に有し、

前記送信手段は、前記デジタル署名を更に含む送信メッセージを生成し、

前記受信手段は、前記受信メッセージに含まれる前記相手通信装置のデジタル署名を更に取り出し、

前記表示手段は、前記相手通信装置のデジタル署名を復号し、前記ハッシュ関数手段でハッシュ関数を実行してメッセージの正当性を確認できた場合に、前記受信手段が取り出した前記相手通信装置を識別するためのID情報と、前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報とを表示する

ことを特徴とする請求項8記載の通信装置。

【請求項10】

前記通信路を特定する情報は、伝送に使用された無線チャネル情報である

ことを特徴とする請求項8または9記載の通信装置。

【請求項11】

前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報は、前記相手通信装置の公開鍵情報であり、

前記送信手段が送信メッセージを送信する際の通信路を特定する情報は、自装置の公開鍵情報である

ことを特徴とする請求項8または9記載の通信装置。

【請求項12】

前記送信手段は、前記暗号化手段によって前記相手通信装置の公開鍵を使用して暗号化された送信メッセージを送信する

ことを特徴とする請求項8または9記載の通信装置。

【請求項13】

乱数を発生させる疑似乱数発生手段を更に有し、

前記送信手段は、前記自装置を識別するためのID情報として前記疑似乱数発生手段で生成した乱数を使用する

ことを特徴とする請求項8または9記載の通信装置。

【請求項14】

入力されたデータを用いて演算を行い、共通秘密鍵を生成する共通秘密鍵生成手段を更に有し、

前記共通秘密鍵生成手段は、前記相手通信装置が送信した送信メッセージに含まれる乱数を用いて、前記共通秘密鍵を生成する

ことを特徴とする請求項8または9記載の通信装置。

【発明の名称】 通信方法及び通信装置

【技術分野】

【0001】

本発明は無線LANの接続における第三者装置の不正侵入と攻撃を防ぐのに適した認証と鍵生成の方法及び装置に関するものである。

【背景技術】

【0002】

無線LAN接続においては、有線LANのように繋ぐだけで接続完了となることなく、セキュリティに関する設定も必須な項目である。無線LAN接続のセキュリティ規格であるIEEE Std 802.11iでは、認証と鍵生成という二つの部分からなる接続処理が規定されており、クライアントと認証サーバまたはアクセスポイント（Access Point）が予め認証用の共通情報をもっていることが前提となる。しかし、こうした共通情報を設定するのは一般のユーザにとっては複雑で難しい。また、認証サーバを設置・設定するとすればユーザにとって非常に手間がかかる。

【0003】

IEEE Std 802.11iでは、認証の基本手順を定義しているが、それを認証サーバが普段設置されていない家庭内のネットワークを適用すると、クライアントとアクセスポイントで共通鍵または相手の公開鍵を予め共有しないため、認証段階において、無線通信でID情報に対して認証を行う際にも、第三者装置による盗聴、成りすましを防ぐことはできない（非特許文献1参照）。

【非特許文献1】 IEEE Std 802.11i/D3.0, November 2002

【発明の開示】

【発明が解決しようとする課題】

【0004】

以上述べたように、従来の方法では、認証用情報の共有段階において交換される認証要求と認証応答というメッセージは第三者装置（Man-in-the-Middle）によって盗聴・改竄される可能性がある。具体的には以下に説明する。

【0005】

認証を行う前に、クライアントとアクセスポイントは事前、共通秘密鍵と相手の証明書をもっていないので、認証と鍵生成のために、自身の公開鍵を相手に通知することが必要となる（図2）。それを無線で送信するので、第三者によって簡単に盗聴されてしまう。

【0006】

第三者装置は、公開鍵を取り替えることにより、クライアント側に対して、電波強度操作により、自分は本当のアクセスポイントのように、アクセスポイント側に対して自分は本当のクライアントのように装うこと（図3）を、クライアントもアクセスポイントもユーザも全然感知しない。

【0007】

無線LANでは、電波を伝送メディアとするので、人間にとってはそれが見えないものであり、それを利用した第三者装置は、チャンネルを変えてメッセージを転送し、送信元に転送することを隠すことができる。

【0008】

認証の手順が破れると、鍵生成もセキュアでなくなる。

【0009】

本発明は、前記従来の課題を解決するもので、認証用共通情報の設定を簡単化しながら、認証用情報の共有段階において第三者による盗聴となりすましを防ぐことで、認証と鍵生成をよりセキュアにする方法を提供することを目的とする。

【課題を解決するための手段】

【0010】

前記第1の通信装置と前記第2の通信装置との間で認証処理を行った上で前記第1の通信装置と前記第2の通信装置との間で通信を行う通信方法であって、前記第2の通信装置の公開鍵情報と、前記第2の通信装置を特定するためのID情報とを含む認証要求メッセージを前記第1の通信装置に送信する認証要求ステップと、前記第1の通信装置が受信した前記認証要求メッセージに含まれる、前記第2の通信装置を特定するためのID情報と、前記認証要求メッセージを受信した際の通信路を特定する情報とを表示する第1の表示ステップと、前記第2の通信装置が送信した前記認証要求メッセージに含まれる、前記第2の通信装置を特定するためのID情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とを表示する第2の表示ステップと、前記第1の表示ステップと、前記第2の表示ステップで表示された前記第2の通信装置を特定するためのID情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とが一致しているかどうかを確認する第1の確認ステップと、前記第1の確認ステップにおいて、前記第2の通信装置を特定するためのID情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とが一致していると判断した場合に、前記第1の通信装置の公開鍵情報と、前記第1の通信装置を特定するためのID情報とを含む認証応答メッセージを前記第2の通信装置に送信する認証応答ステップと、前記第2の通信装置が受信した前記認証応答メッセージに含まれる、前記第1の通信装置を特定するためのID情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する第3の表示ステップと、前記第1の通信装置が送信した前記認証応答メッセージに含まれる、前記第1の通信装置を特定するためのID情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示する第4の表示ステップと、前記第3の表示ステップと、前記第4の表示ステップで表示された前記第1の通信装置を特定するためのID情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とが一致しているかどうかを確認する第2の確認ステップとで構成されることを特徴とする。

【0011】

また、請求項2における発明は、請求項1に記載の通信方法において、前記認証要求ステップにおいて、認証要求メッセージはデジタル署名情報を更に含み、前記第1の表示ステップにおいて、前記認証要求メッセージに含まれるデジタル署名情報を復号した結果、前記第2の通信装置の署名であると確認した場合に、前記第2の通信装置を特定するためのID情報と、前記認証要求メッセージを送信する際の通信路を特定する情報とを表示し、前記認証応答ステップにおいて、認証応答メッセージはデジタル署名情報を更に含み、前記第3の表示ステップにおいて、前記認証応答メッセージに含まれるデジタル署名情報を復号した結果、前記第1の通信装置の署名であると確認した場合に、前記第1の通信装置を特定するためのID情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とを表示することを特徴とする。

【0012】

また、請求項3における発明は、請求項1または2に記載の通信方法において、前記認証要求メッセージを送信する際の通信路を特定する情報及び、前記認証応答メッセージを送信する際の通信路を特定する情報は、伝送に使用された無線チャネル情報であることを特徴とする。

【0013】

また、請求項4における発明は、請求項1または2に記載の通信方法において、前記認証要求メッセージを送信する際の通信路を特定する情報は、前記第2の通信装置の公開鍵情報であり、前記認証応答メッセージを送信する際の通信路を特定する情報は、前記第1の通信装置の公開鍵情報であることを特徴とする。

【0014】

また、請求項5における発明は、請求項1または2に記載の通信方法において、前記認証応答ステップにおいて、前記認証応答メッセージを前記第2の通信装置の公開鍵情報で暗号化することを特徴とする。

【 0 0 1 5 】

また、請求項 6 における発明は、請求項 1 または 2 に記載の通信方法において、前記第 1 の通信装置を特定するための ID 情報及び前記第 2 の通信装置を特定するための ID 情報は、通信路設定を行うたびに都度生成する乱数であることを特徴とする。

【 0 0 1 6 】

また、請求項 7 における発明は、請求項 1 または 2 に記載の通信方法において、前記第 2 の確認ステップにおいて、前記第 1 の通信装置を特定するための ID 情報と、前記認証応答メッセージを送信する際の通信路を特定する情報とが一致していると判断した場合に、前記第 2 の通信装置が、自身の生成した乱数を含む共通秘密鍵生成要求メッセージを前記第 1 の通信装置に送信する共通秘密鍵生成要求ステップと、前記共通秘密鍵生成要求メッセージを受信した前記第 1 の通信装置が、自身の生成した乱数を含む共通秘密鍵生成応答メッセージを前記第 2 の通信装置に送信する共通秘密鍵生成応答ステップと、前記第 1 の通信装置が、前記共通秘密鍵生成要求メッセージに含まれる乱数を用いて演算を行い、共通秘密鍵を生成し、前記第 2 の通信装置が、前記共通秘密鍵生成応答メッセージに含まれる乱数を用いて演算を行い、共通秘密鍵を生成する共通秘密鍵生成ステップを更に含むことを特徴とする。

【 0 0 1 7 】

また、請求項 8 における発明は、相手通信装置との間で認証処理を行った上で前記相手通信装置との間で通信を行う通信装置であって、自装置の公開鍵及びプライベート鍵ペアを作成する公開鍵・プライベート鍵生成手段と、前記公開鍵・プライベート鍵作成手段が生成した公開鍵情報と、自装置を識別するための ID 情報とを少なくとも含む送信メッセージを生成し、前記相手通信装置に送信する送信手段と、前記相手通信装置が送信した送信メッセージを受信し、前記相手通信装置が送信した送信メッセージに含まれる前記相手通信装置の公開鍵情報と、前記相手通信装置を識別するための ID 情報とを取り出す受信手段と、自装置が前記相手通信装置から送信メッセージを受信した場合、前記受信手段が取り出した前記相手通信装置を識別するための ID 情報と、前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報とを表示する機能と、自装置が前記相手通信装置に送信メッセージを送信した場合、自装置が送信した送信メッセージに含まれる、自装置を特定するための ID 情報と、前記送信手段が送信メッセージを送信する際の通信路を特定する情報とを表示する機能とを有する表示手段と、認証を許可するかどうかを入力する入力手段とを有することを特徴とする。

【 0 0 1 8 】

また、請求項 9 における発明は、請求項 8 に記載の通信装置において、入力されたデータを暗号化し、その結果をデジタル署名として出力するデジタル署名手段と、前記相手通信装置から受信した前記相手通信装置の公開鍵、或いは自装置のプライベート鍵、或いは前記相手通信装置と共有する共通秘密鍵を用いて入力されたデータを暗号化する暗号化手段と、前記相手通信装置から受信した前記相手通信装置の公開鍵、或いは自装置のプライベート鍵、或いは前記相手通信装置と共有する共通秘密鍵を用いて入力されたデータを復号化する復号化手段と、入力されたデータに対して一方向ハッシュ関数を実行するハッシュ関数手段を更に有し、前記送信手段は、前記デジタル署名を更に含む送信メッセージを生成し、前記受信手段は、前記受信メッセージに含まれる前記相手通信装置のデジタル署名を更に取り出し、前記表示手段は、前記相手通信装置のデジタル署名を復号し、前記ハッシュ関数手段でハッシュ関数を実行してメッセージの正当性を確認できた場合に、前記受信手段が取り出した前記相手通信装置を識別するための ID 情報と、前記受信手段が前記送信メッセージを受信した際の通信路を特定する情報とを表示することを特徴とする。

【 0 0 1 9 】

また、請求項 10 における発明は、請求項 8 または 9 に記載の通信装置において、前記通信路を特定する情報は、伝送に使用された無線チャネル情報であることを特徴とする。

【 0 0 2 0 】

また、請求項 11 における発明は、請求項 8 または 9 に記載の通信装置において、前記

又は子機が前記返信メッセージを返信した際の返信時を付与する情報は、前記相手通信装置の公開鍵情報であり、前記送信手段が送信メッセージを送信する際の通信路を特定する情報は、自装置の公開鍵情報であることを特徴とする。

【0021】

また、請求項12における発明は、請求項8または9に記載の通信装置において、前記送信手段は、前記暗号化手段によって前記相手通信装置の公開鍵を使用して暗号化された送信メッセージを送信することを特徴とする。

【0022】

また、請求項13における発明は、請求項8または9に記載の通信装置において、乱数を発生させる疑似乱数発生手段を更に有し、前記送信手段は、前記自装置を識別するためのID情報として前記疑似乱数発生手段で生成した乱数を使用することを特徴とする。

【0023】

また、請求項14における発明は、請求項8または9に記載の通信装置において、入力されたデータを用いて演算を行い、共通秘密鍵を生成する共通秘密鍵生成手段を更に有し、前記共通秘密鍵生成手段は、前記相手通信装置が送信した送信メッセージに含まれる乱数を用いて、前記共通秘密鍵を生成することを特徴とする。

【発明の効果】

【0024】

本発明によれば、第三者装置（Man-in-the-Middle）がクライアントとアクセスポイント間の接続設定時に交換されるメッセージへの盗聴またはなりすまし、更にクライアントやアクセスポイントに対する乗っ取りなど悪行為を防ぐことができる。

【0025】

また、本発明によれば、認証と鍵交換を同時に行うので、クライアントとアクセスポイントで共通鍵または公開鍵の交換または事前共有することが必要でなくなる。

【0026】

なお、本発明によれば、認証直後に、認証時に交換された公開鍵を使用して、共通秘密鍵をセキュアに生成することができる。

【0027】

なお、本発明を他の方式の有線・無線のネットワークに適用することも可能であり、第三者攻撃を防げるという本発明の効果が得られる。

【発明を実施するための最良の形態】

【0028】

以下本発明の実施の形態について、図面を参照しながら説明する。

【0029】

まず、全体的な構成及び各部分の機能を説明する。図1は、認証と鍵生成のために必要とされる機能モジュール構成を示す。このモジュールは、アクセスポイント（AP）とクライアント両方ともに実装される。認証部10は、初期化のほかに各モジュールを含め全体的にコントロールする役割を果たす。クライアントはAPに（初）接続されると、このモジュールが起動され、認証が開始する。それから、以後に述べる手順に基づいて、イベント処理やモジュールの呼び出しと後続処理を行う。また、認証要求メッセージの第三者装置による改竄・転送への監視とチャンネル情報表示または公開鍵表示等のコントロールも行う。認証部10は、無線LANカードに乗せられる。

【0030】

公開鍵・プライベート鍵生成部11は、自身の公開鍵・プライベート鍵ペアを生成する機能を有し、機器が起動された際に呼び出され、公開鍵・プライベート鍵を生成する。

【0031】

デジタル署名部12は、ハッシュ関数部16を用いて、メッセージを固定長に短縮し、前記プライベート鍵で暗号化部13のアルゴリズムを呼び出して暗号化し、暗号化した結果をデジタル署名として前記メッセージに付け加える。

【0032】

暗号化部 13 は、相手の公開鍵または自身のプライベート鍵または相手と共有する共通秘密鍵を用いて暗号化するためのアルゴリズムを含む。

【0033】

復号部 14 は、相手の公開鍵または自身のプライベート鍵または相手と共有する共通秘密鍵を用いて復号するためのアルゴリズムを含む。

【0034】

擬似乱数発生部 15 は、規則性を予測しにくい擬似乱数生成機能を有し、ノンスや（必要な時）ID を生成するためのモジュールである。

【0035】

ハッシュ関数部 16 は、長いビット列を固定長のビット列に圧縮する一方向ハッシュ関数を含む。

【0036】

共通秘密鍵生成部 17 は、二つのノンス（乱数）に基づき、擬似乱数発生部 15 を用いて秘密鍵を生成するモジュールである。

【0037】

送信部 18 は、認証部 10 から必要な情報を取得し、送信メッセージを組み立てると共に、MAC レイヤでメッセージの送信をコントロールし、送信に使用されたチャンネルの情報（例えば、チャンネル番号）を前記認証部 10 に返す。また、自機器を特定するための ID 情報（例えば、機器に設定された名前や MAC アドレス）を保持する。

【0038】

受信部 19 は、MAC レイヤでメッセージの受信をコントロールし、受信メッセージから必要な情報を取り出して認証部 10 に渡す。また、受信に使用されたチャンネルの情報（例えば、チャンネル番号）を前記認証部 10 に返す。

【0039】

表示部 20 は、送受信に伴って、ID 情報とチャンネル情報または公開鍵を表示する装置であって、ユーザに確認して認証許可判断を行なわせる。

【0040】

入力部 21 は、ユーザの認証許可判断を入力させるために備えた装置（例えば、ボタン）である。

【0041】

前記公開鍵・プライベート鍵生成部 11、デジタル署名部 12、暗号化部 13、復号部 14、擬似乱数発生部 15、ハッシュ関数部 16、共通秘密鍵生成部 17 は、図 1 のように認証部の内部モジュールとして認証部と一体になって実装してもよいし、個別的に認証部の外に置いてまたは使用可能な外部共通モジュールを呼び出して使用するという形での実装でもよい。

【0042】

次に、認証と鍵生成に関する手順の実施について説明する。

【0043】

（実施の形態 1）

図 4 に、クライアント 2 を AP 1 に接続する際に、本発明による接続の手順を示す。プローブ要求 300 は、従来標準のフォーマットを採用する。プローブ応答 301 は、従来のプローブ応答のサポートできる接続方式リストに本発明の接続方式を追加したフォーマットを採用する。プローブ確認 302 は、従来標準ではなく、本発明の接続方式を行うこととそれに必要なパラメータを知らせる機能を持つ新しいメッセージタイプである。認証要求 303 以降のメッセージは全て本発明規定の新しいフォーマットを採用する。認証要求 303 のフォーマットを図 5 に示す。HDRc 1001 はクライアント 2 のアドレスやメッセージタイプを含むヘッダーであり、従来の認証要求のヘッダーと同様である。PLc 1002 は従来と同じようなペイロードである。PKc 1003 は前記クライアント 2 の公開鍵である。IDc 1004 は前記クライアント 2 の ID である。SIGNc 1005 は、ヘッダーをはじめ全てのフィールドに対して前記クライアント 2 のデジ

ノル番部12を用いて署名したものである。クライアント2の返信部10は、公開鍵・プライベート鍵生成部11からクライアント2の公開鍵PKc 1003を取得する。また、デジタル署名部12からSIGNc 1005を取得し、送信部18が保持するIDc 1004と合わせて認証要求303を生成する。認証要求303によって、クライアント2の公開鍵PKcをAP1に渡すことが出来る。

【0044】

クライアント2が認証要求303を送信し、クライアント2自身の表示部20に、IDcと自身の送信部18で送信に使用されたチャンネルの情報（例えば、無線チャンネル番号）を表示する。

【0045】

AP1が認証要求303を受信すると、AP1の受信部19は認証要求303に含まれるクライアント2の公開鍵PKc 1003と、デジタル署名SIGNc 1005を取り出し、AP1の認証部10に渡す。クライアント2の公開鍵PKc 1003とAP1自身の復号部14を用いてSIGNc 1005を復号した結果を、受信した認証要求303に対し、AP1のハッシュ関数部16で自身のハッシュ関数を用いて、クライアント2の署名時に使用した同じハッシュ関数を掛けた結果と比較し（即ち、完全性チェックを行い）、一致したら、受信した認証要求303に含まれたIDと、AP1の受信部19で受信に使用されたチャンネルの情報（例えば、無線チャンネル番号）をAP1自身の表示部20に表示する。ユーザが、クライアント2の表示部20に表示されているID及びチャンネル情報と、AP1の表示部20に表示されているID及びチャンネル情報とが一致するかしないかを確認し、一致したら、認証許可をAP1の入力部21を用いて行う。

【0046】

なお、本実施の形態では、デジタル署名SIGNcを復号し、完全性を確認できた場合に、受信した認証要求に含まれたIDと、受信部で受信に使用されたチャンネルの情報をAP1自身の表示部20に表示しているが、デジタル署名を使用せず、受信した認証要求の内容を無条件に表示し、一致を確認しても良い。

【0047】

前記認証要求を行う際に、図3のように第三者装置3が入り込んでしまうと、クライアント2から送信された認証要求は、第三者装置3に盗聴されて、そのまま転送されるか、または、第三者装置3が受信した認証要求303に対して、図8に示すように、公開鍵PKc 1003を自身の公開鍵PKm 1303に取り替えて、また、署名SIGNc 1005も自身のプライベート鍵による署名SIGNm 1305に取り替えて、こうして改竄した認証要求402をAP1へ送出するかということがあるが、何れクライアント2またはAP1の監視によって検知される。検知された結果を表示部に表示し、認証中断とする。第三者装置3が傍受しているだけの場合は、理解できるのは暗号化していない前記認証要求または後の認証応答だけであり、それ以降にやりとりされるメッセージは、交換した公開鍵PKc及びPKaで暗号化される。このため、認証に対して悪影響をもたらそうとするのはこの認証方法により不可能である。また、第三者装置3が、クライアント2の送信に使用された送信チャンネルを異なったチャンネルで転送した場合は、前記クライアント2とAP1の表示部に表示されたチャンネル情報の一致性確認によって検知される。

【0048】

前記認証要求が成功した場合、AP1からクライアント2へ認証応答305を返信する。認証応答305のフォーマットを図6に示す。PLa 1102は認証結果を含む。PKa 1103はAP1の公開鍵である。IDa 1104はAP1のIDである。SIGNa 1105は、AP1のプライベート鍵とデジタル署名部を用いて認証応答305の各フィールドに対する署名である。AP1の送信部18は、公開鍵・プライベート鍵生成部11からクライアント1の公開鍵PKa 1103を取得する。また、デジタル署名部12からSIGNa 1105を取得し、送信部18が保持するIDa 1104と合わせて認証応答305を生成する。認証応答305によって、AP1の公開鍵PKaをク

クライアント2に送りこくが山なる。

【0049】

AP1が認証応答305を送信した後、AP1自身の送信部18で送信に使用されたチャンネルの情報（例えば、無線チャンネル番号）とIDaをAP1自身の表示部20に表示し、認証応答305を第三者装置に改竄・転送されるのを監視する。

【0050】

クライアント2が認証応答305を受信すると、クライアント2の受信部19は、認証応答305に含まれるAP1の公開鍵PKa 1103と、デジタル署名SIGNa 1105を取り出し、クライアント2の認証部10に渡す。そして、AP1と同様の方法でメッセージの完全性をチェックする。完全性に問題がなければ、受信した認証応答305に含まれたIDと、クライアントの受信部19で受信に使用されたチャンネルの情報（例えば、チャンネル番号）をクライアント2自身の表示部20に表示する。ユーザが、クライアント2の表示部20とAP1の表示部20とに表示されているIDとチャンネル情報とをそれぞれ確認し、一致したら、認証許可をクライアント2の入力部21を用いて行い、認証成功となる。

【0051】

（実施の形態2）

認証要求メッセージが第三者装置に改竄・転送されることに対する監視を、クライアント2またはAP1が行う。クライアント2が行うのが、第三者装置の送信したメッセージ全てをクライアント2が受信できる状況にある場合に有効である。AP1が行うのが、クライアント2の送信したメッセージと第三者装置の送信したメッセージ全てをAP1が受信できる状況にある場合に有効である。クライアント2が行う場合は、AP1からの認証応答が返信されるまでに受信した第三者装置の改竄した認証要求は、含まれた公開鍵と署名を除いて自身の送出した認証要求と同じであれば、第三者装置の改竄・転送行為を断定する。AP1が行う場合は、一定時間内に公開鍵と署名を除いて全く同じ認証要求を二つ受信すれば、第三者装置の改竄・転送行為を断定する。AP1が図8に示すような認証応答402を受信したら、公開鍵PKm 1303と署名SIGNm 1305を除いて同じ認証応答を二つ受信しているか、クライアント2も自身が送信した認証要求の公開鍵と署名を改竄されたこの認証要求を受信しているかになるので、どちらかで第三者装置の改竄・転送を断定できる。

【0052】

認証応答メッセージが第三者装置に改竄・転送されることに対する監視・断定は、前記認証要求メッセージと同じような処理の仕方を用い、クライアント2とAP1と役割を交換すればよい。クライアント2が図9に示すような認証応答404を受信したら、公開鍵PKm 1403と署名SIGNm 1405を除いて同じ認証応答を二つ受信しているか、AP1も自身が送信した認証応答の公開鍵と署名を改竄されたこの認証応答を受信しているかになるので、どちらかで第三者装置の改竄・転送を断定できる。

【0053】

（実施の形態3）

認証要求メッセージまたは認証応答メッセージを第三者装置に改竄・転送されることを断定するために、監視とチャンネル情報表示という手法を使用するのではなく、認証要求メッセージまたは認証応答メッセージに含まれる公開鍵を表示して、クライアント2の表示部20とAP1の表示部20に表示された公開鍵の一致性をユーザに確認させ、認証許可を行わせる。

【0054】

公開鍵は長いので、表示部に一遍で表示し切れない場合は、ハッシュ関数部16を用いて短縮して表示するか、図示しないスイッチを設けて表示部20と連動させ、スライドで表示させてもよい。

【0055】

（実施の形態4）

認証応答305は図10に示すようなフォーマットを採用する。AP1の暗号化部13が、認証応答情報PLa 1202、AP1の公開鍵PKa 1203、AP1のIDa 1204を、認証要求303で受け取ったクライアント2の公開鍵PKcで暗号化して、認証応答305をクライアント2に送信する。このような認証応答305は、公開鍵PKcのペアであるプライベート鍵をもつクライアント2しか復号できない。なお、このような認証応答305を使用した場合は、IDとチャンネル情報または公開鍵PKcの表示と確認を行う必要がなくなる。

【0056】

なお、この場合は、認証要求を行う段階で第三者装置の改竄はないと確認できたので、クライアント2またはAP1が図10に示すような認証応答404を受信することはない。第三者装置がこの段階からこのような認証応答を使用して攻撃しても、クライアント2にただ無視され、悪影響にはならない。

【0057】

(実施の形態5)

クライアント2またはAP1のIDとして、クライアントの接続を行う都度にクライアント2及びAP1の擬似乱数発生部15で生成した乱数を使用する。これは、MACアドレスや製品の型番より、より高い秘密性を持つ。ユーザ定義の名前をIDとしてここで使うことも可能であるが、事前、入力しておく手間がかかり、且つ、ユーザはなるべくユニーク（特に隣家の同様な機器と異なるよう）な名前を設定しなければならない。乱数を使用することで、次回接続時には、違うIDになるので、盗まれても問題はない。

【0058】

(実施の形態6)

認証に成功した場合、クライアント2は、AP1へ図11に示すような共通秘密鍵生成要求307を送信する。共通秘密鍵生成要求307は、ヘッダーHDRc 1601を除いた部分がクライアント2の暗号化部13においてAP1の公開鍵PKaを用いて暗号化される。IDc 1602はクライアント2のIDである。Nc 1603はクライアント2が生成したノンス（乱数）である。クライアント2の暗号化部13は、クライアント2の送信部18が保持するIDcと、クライアント2の擬似乱数発生部15が生成したノンス（乱数）Ncを取得し、暗号化する。クライアント2の送信部18は、暗号化されたIDcと、ノンス（乱数）NcにヘッダーHDRc 1601を付加し、共通秘密鍵生成要求307を送信する。AP1の受信部19が、共通秘密鍵生成要求307を受信し、復号の対象となるデータを取り出して復号部14に渡す。復号部14において、自身のプライベート鍵で復号する。復号結果において、IDは先に認証したクライアント2のIDcであることを確認する。確認できたら、復号結果で得られたNcを取っておき、後の鍵生成に用いる。そうでなければ、受信した共通秘密鍵生成要求307を廃棄し、鍵生成を中止とする。

【0059】

AP1が、共通秘密鍵生成要求307を正確に受信し且つ確認できた場合には、クライアント2に、図12に示すような共通秘密鍵生成応答308を返信する。共通秘密鍵生成応答308は、ヘッダーHDRa 1701を除いた部分がクライアント2の公開鍵PKcを用いて暗号化される。IDa 1702はAP1のIDである。Na 1703はAP1が生成したノンス（乱数）である。AP1の暗号化部13は、AP1の送信部18が保持するIDaと、AP1の擬似乱数発生部15が生成したノンス（乱数）Naを取得し、暗号化する。AP1の送信部18は、暗号化されたIDaと、ノンス（乱数）NaにヘッダーHDRa 1701を付加し、共通秘密鍵生成応答308を送信する。クライアント2の受信部19が、共通秘密鍵生成応答308を受信し、復号の対象となるデータを取り出して復号部14に渡す。復号部14において、自身のプライベート鍵で復号する。復号結果において、IDは先に認証したAP1のIDaであることを確認する。確認できたら、復号結果で得られたNaを取っておき、後の鍵生成に用いる。そうでなければ、受信した共通秘密鍵生成応答308を廃棄し、鍵生成を中止とする。

【 0 0 6 0 】

鍵生成は、AP 1 及びクライアント 2 の共通秘密鍵生成部 1 7 において、Nc と Na 及び次の式に基づいて行う。鍵 = prf (PreMasterKey, " control " || IDADDRc || IDADDRa || Nc || Na) 。但し、prf は擬似乱数関数である。PreMasterKey はこの発明の実施にあたって内部で設定した共通な数値である。IDADDRc はクライアント 2 の ID または MAC アドレス、IDADDRa は AP 1 の ID または MAC アドレスである。Nc と Na は、前記認証時に交換されたクライアントと AP のノンズである。これで、AP 1 とクライアント 2 は、同じ鍵を生成し、共有することになる。

【 0 0 6 1 】

クライアント 2 と AP 1 が生成した前記共通秘密鍵を、次のアソシエーションの作成に用いる。つまり、図 4 のアソシエーション要求 3 0 9 もアソシエーション応答 3 1 0 も、この鍵を用いて暗号化される。一方、受信側は、この鍵を用いて受信したメッセージを復号する。

【 0 0 6 2 】

前記生成した鍵は、クライアント 2 と AP 1 間のコントロールメッセージの送受信に用いるが、データ送受信のために別の鍵を用いてもよい。その場合は、鍵 = prf (PreMasterKey, " data " || IDADDRc || IDADDRa || Nc || Na) という式を用いて生成する。

【 0 0 6 3 】

以上の文章と図の中には、クライアントとアクセスポイントとの間の認証と鍵生成に関するアーキテクチャのみ記述した。しかし、実際には、アクセスポイントの向こうがルータ或いはホームゲートウェイの場合は、アクセスポイントをルータ或いはホームゲートウェイに代わってクライアントとの認証・鍵生成を行ってもよい。つまり、クライアントの認証と鍵生成の相手は、ルータあるいはホームゲートウェイになる。但し、この場合には、ルータ或いはホームゲートウェイは、アクセスポイントとセキュアな通信経路で繋がれており、アクセスポイントは中継機能を果たす。なお、本発明は、ルータ或いはホームゲートウェイとアクセスポイントとの間に無線 LAN で繋ぐ場合の接続にも応用できる。

【産業上の利用可能性】

【 0 0 6 4 】

本発明の提案したセキュリティ強度を高めた接続方法は、第三者 (Man-in-the-Middle) 攻撃を予防・排除できる特徴を有し、無線 LAN の目視認証及び鍵生成をよりセキュアにする方法として有用である。また、第三者攻撃が存在しうる他のタイプの有線・無線ネットワークにおける相互認証と鍵生成にも応用できる。

【図面の簡単な説明】

【 0 0 6 5 】

【図 1】 本発明の機能モジュール構成図

【図 2】 従来の無線 LAN における目視確認での接続処理の流れ図

【図 3】 第三者装置 (Man-in-the-Middle) が侵入した場合の状況図

【図 4】 本発明の接続処理の流れ図

【図 5】 本発明の認証要求メッセージのフォーマット図

【図 6】 本発明の認証応答メッセージのフォーマット図 (案 1)

【図 7】 本発明の認証応答メッセージのフォーマット図 (案 2)

【図 8】 第三者装置によって改竄・転送された認証要求メッセージのフォーマット図

【図 9】 第三者装置によって改竄・転送された認証応答メッセージのフォーマット図 (案 1)

【図 1 0】 第三者装置によって改竄・転送された認証応答メッセージのフォーマット図 (案 2)

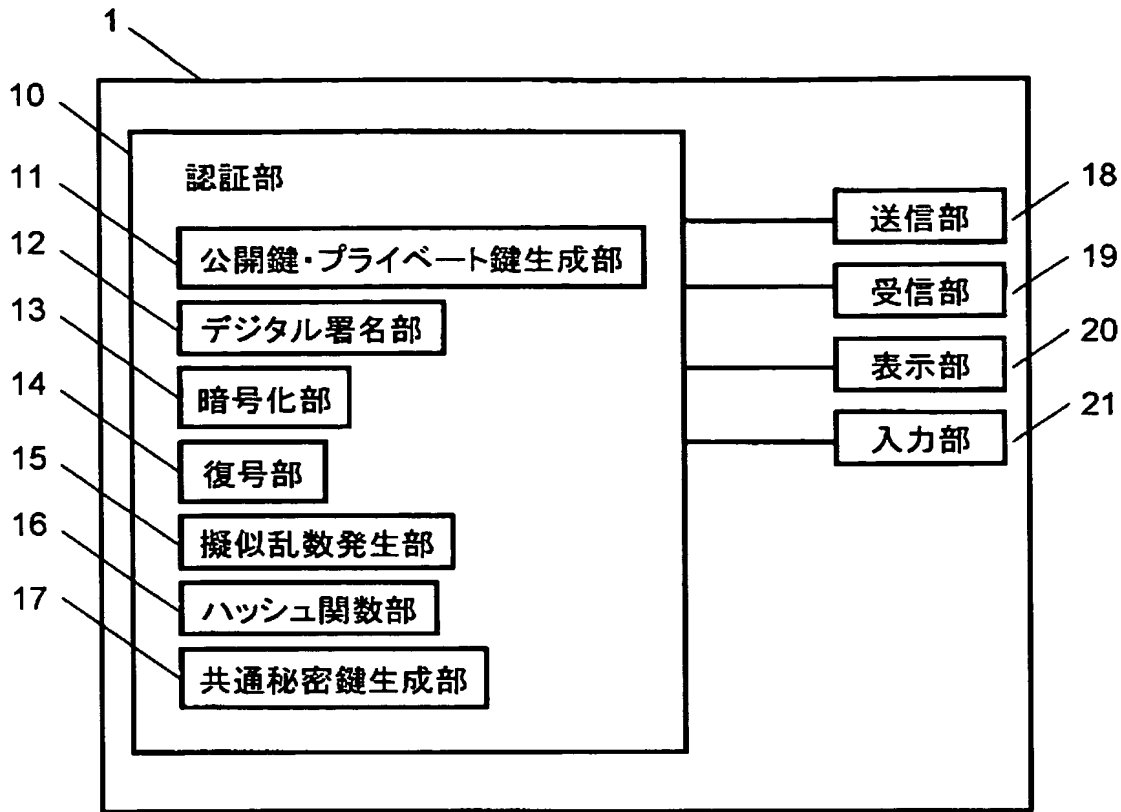
【図 1 1】 本発明の共通秘密鍵生成要求メッセージのフォーマット図

【符号の説明】

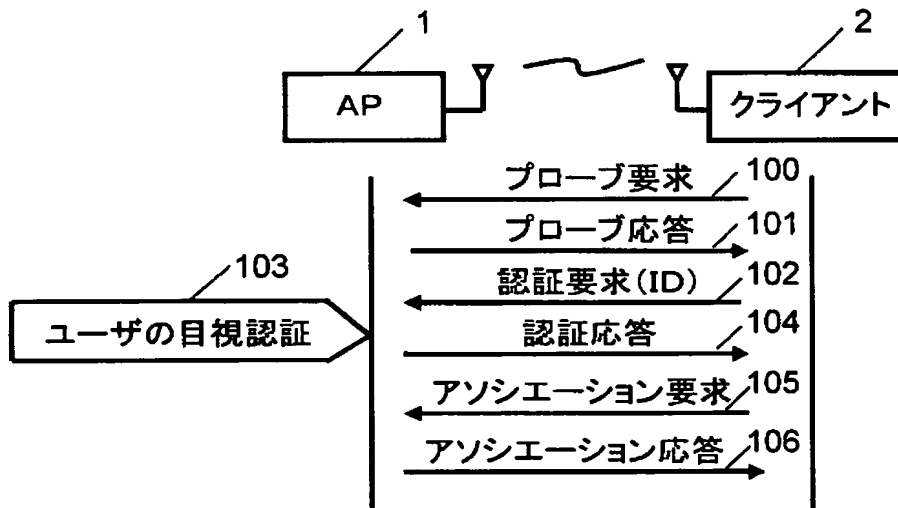
【 0 0 6 6 】

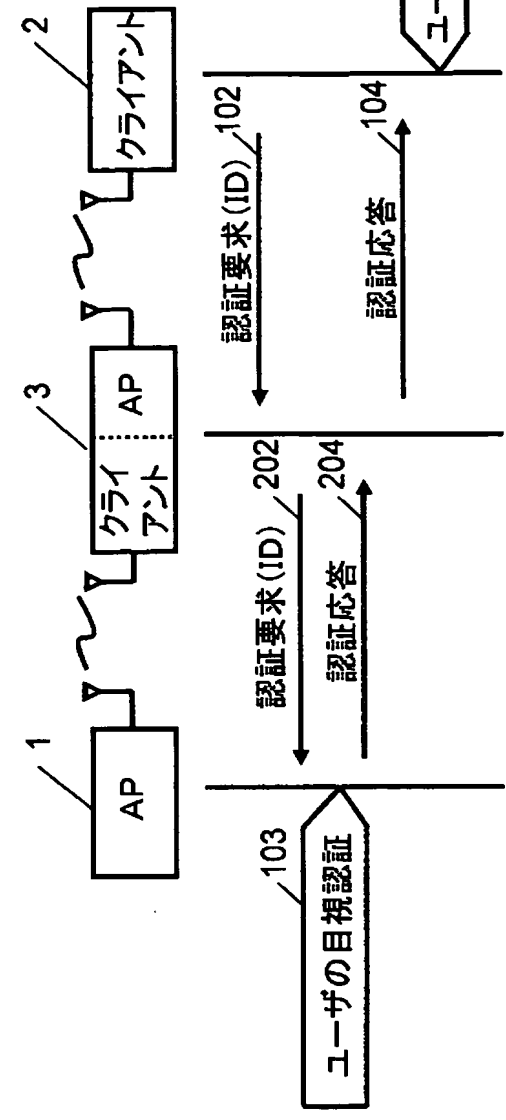
- 1 認証・鍵生成機能ブロック
- 1 0 認証部
- 1 1 公開鍵・プライベート鍵生成部
- 1 2 デジタル署名部
- 1 3 暗号化部
- 1 4 復号部
- 1 5 疑似乱数発生部
- 1 6 ハッシュ関数部
- 1 7 共通秘密鍵生成部
- 1 8 送信部
- 1 9 受信部
- 2 0 表示部
- 2 1 入力部

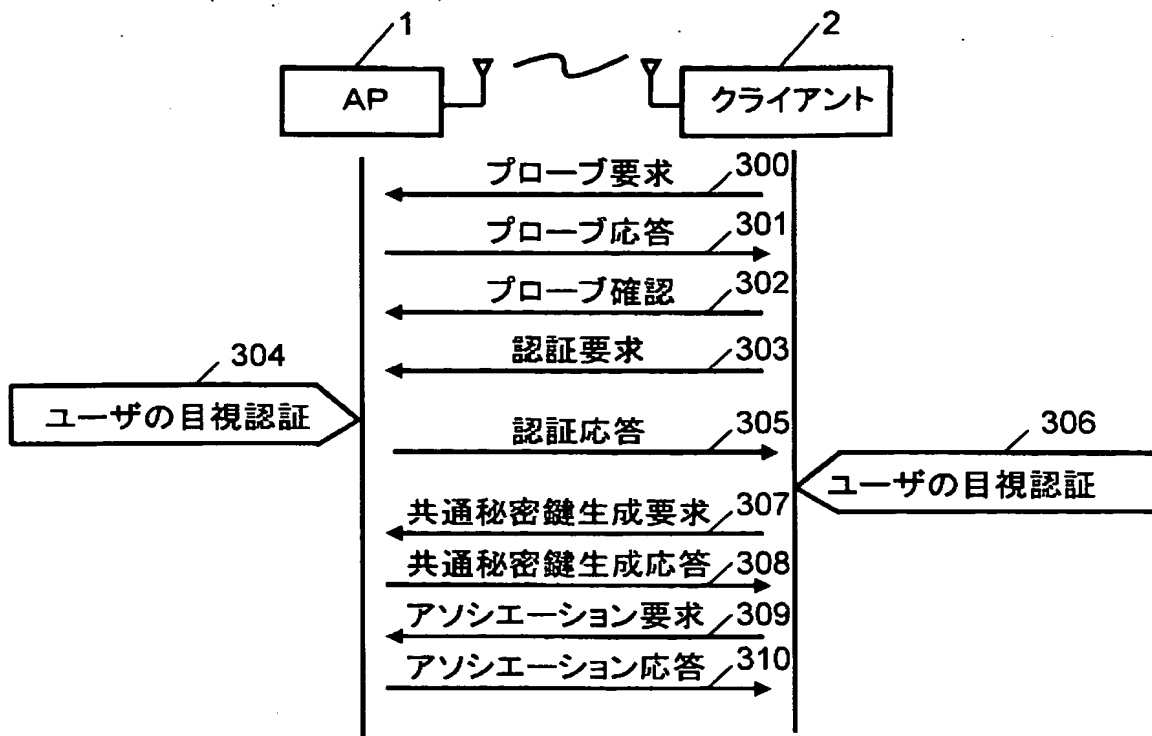
【 図 1 】



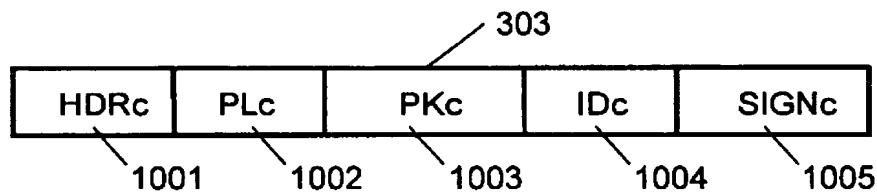
【 図 2 】



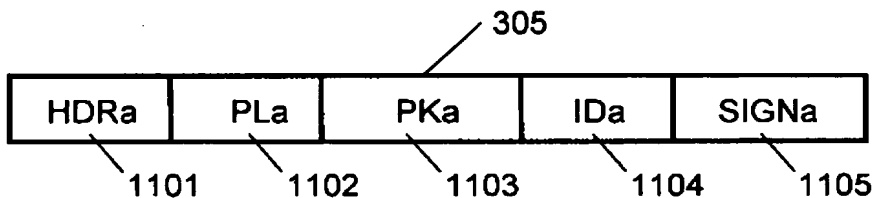




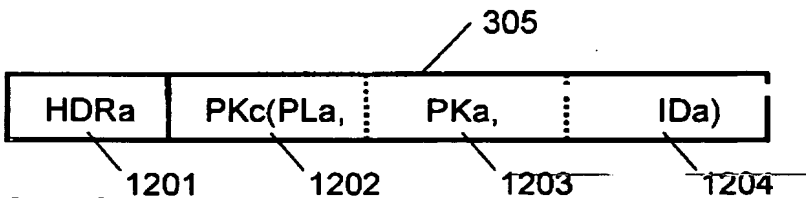
【図 5】



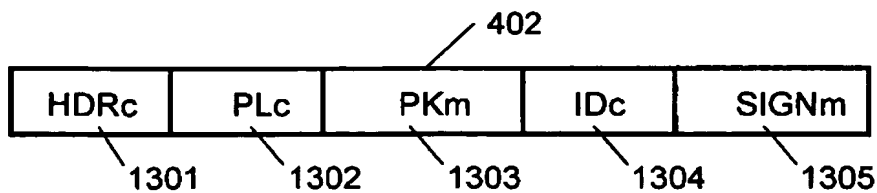
【図 6】

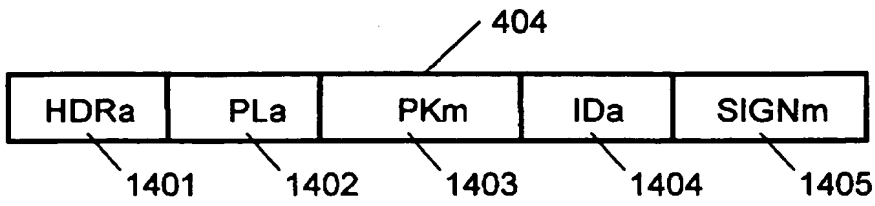


【図 7】

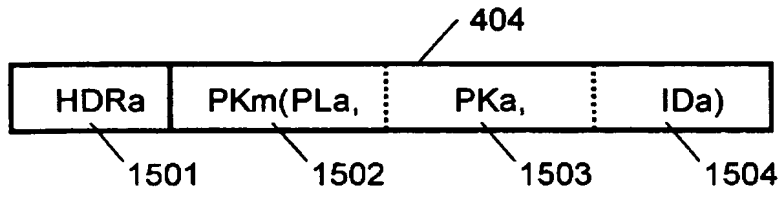


【図 8】

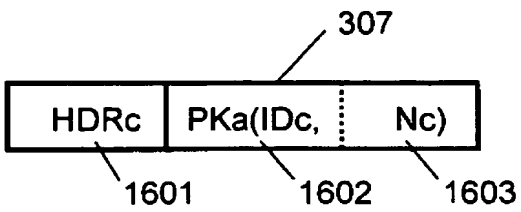




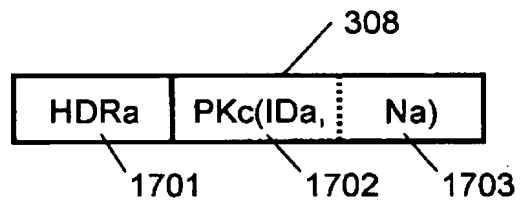
【 図 1 0 】



【 図 1 1 】



【 図 1 2 】



【要約】

- 【課題】無線LANの接続において、共通鍵や証明書を利用しない場合、ユーザは目視で認証するという簡単な方法を用いる際に、第三者（Man-in-the-Middle）による盗聴となりすまし等悪行為を防ぐこと。

【解決手段】公開鍵・プライベート鍵生成部11と、デジタル署名部12と、暗号化部13と、復号部14と、疑似乱数発生部15と、ハッシュ関数部16と、共通秘密鍵生成部17とを備え、認証要求メッセージと認証応答メッセージに公開鍵とIDを加えて、プライベート鍵で署名して、または、公開鍵で暗号化して送信する。受信側は復号して、含まれた情報を表示部20に表示する。ユーザはクライアントとAP間の表示部に表示された情報の一致性を確認して入力部21を通して認証を行う。こうすることにより、第三者装置の盗聴となりすましを防ぎ、両通信装置間の認証と鍵生成はセキュアとなる。

【選択図】 図1

0 0 0 0 0 5 8 2 1

• 19900828

新規登録

大阪府門真市大字門真 1 0 0 6 番地

松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/007096

International filing date: 12 April 2005 (12.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-147422
Filing date: 18 May 2004 (18.05.2004)

Date of receipt at the International Bureau: 02 June 2005 (02.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record.

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.